Requirements Engineering

Description

Presents best practices for security requirements engineering, including processes that are specific to eliciting, specifying, analyzing, and validating security requirements. Example processes include CLASP, SQUARE, and recent work by Nuseibeh et al. Specific techniques that are relevant to security requirements, such as development of misuse/abuse cases and attack trees and specification techniques such as SCR, are also discussed or referenced.

Overview Articles

###	##### ######## ######	Abstract
Security Requirements Engineering	23.05.06 16:17:49	Security requirements are often identified during the system life cycle. However, the requirements tend to be general mechanisms such as password protection, firewalls, virus detection tools, and the like. As a result, security requirements that are specific to the system and that provide for protection of essential services and assets are often neglected. Several approaches to security requirements engineering are described that can help organizations ensure that their products effectively meet security requirements.

Most Recently Updated Articles [Ordered by Last Modified Date]

###	##### ######## ######	Abstract
Requirements Elicitation Case Studies Using IBIS, JAD, and ARM	22.09.06 16:26:00	This article describes a tradeoff analysis that can be done to select a suitable requirements elicitation method and the results of trying three methods in some case studies. It is a companion to the requirements elicitation introduction[1].
Requirements Elicitation Introduction	22.09.06 16:08:56	An area that is largely neglected is that of elicitation methods for

1. daisy:533 (Requirements Elicitation Introduction)

		security requirements engineering. Many organizations, if they use an elicitation method at all, use one that they have previously used for ordinary functional (end-user) requirements. Alternatively they may decide to use a brainstorming approach to identify security requirements. In many cases these methods are not oriented towards security requirements and do not result in a consistent and complete set of security requirements. The resulting system is likely to have more security exposures than it would if the requirements were elicited in a systematic way. In this article we briefly discuss a number of elicitation methods and the kind of tradeoff analysis that can be done to select a suitable requirements elicitation method. Companion case studies can be found in Requirements Elicitation Case Studies[2]. While results may vary from one organization to another, the discussion of our selection process and various methods should be of general use. Requirements elicitation is an active research area, and we expect to see advances in this area in the future. We also would expect that we will be able to begin to measure which methods are most effective for eliciting security requirements. At present, there is little if any data comparing the effectiveness of different methods for eliciting security requirements.
The Common Criteria	05.09.06 16:48:46	The Common Criteria enable an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements. Although the focus of the Common Criteria

2. daisy:532 (Requirements Elicitation Case Studies Using IBIS, JAD, and ARM)

		is evaluation, it presents a standard that should be of interest to those who develop security requirements.
Attack Trees	06.06.06 16:58:28	Requirements engineering for security should respond to the system's anticipated threats and risks. Risk analysis should identify the most critical attacks, and requirements engineering should propose system requirements to mitigate those attack patterns. Attack trees are one approach for describing possible attacks.
Comprehensive Lightweight Application Security Process (CLASP)	05.06.06 14:14:58	The Comprehensive Lightweight Application Security Process (CLASP) is a set of formal practices that can help developers address security concerns throughout the software development life cycle. It is agnostic with respect to development methodology. A CLASP reference guide is available that includes templates, worksheets, checklists, and guidelines. The guide also describes a number of core concepts and principles for creating a secure application design.

All Articles [Ordered by Title]

###	##### ######## #######	Abstract
Attack Trees	06.06.06 16:58:28	Requirements engineering for security should respond to the system's anticipated threats and risks. Risk analysis should identify the most critical attacks, and requirements engineering should propose system requirements to mitigate those attack patterns. Attack trees are one approach for describing possible attacks.
Comprehensive Lightweight	05.06.06 14:14:58	The Comprehensive Lightweight

Application Security Process (CLASP)		Application Security Process (CLASP) is a set of formal practices that can help developers address security concerns throughout the software development life cycle. It is agnostic with respect to development methodology. A CLASP reference guide is available that includes templates, worksheets, checklists, and guidelines. The guide also describes a number of core concepts and principles for creating a secure application design.
Requirements Elicitation Case Studies Using IBIS, JAD, and ARM	22.09.06 16:26:00	This article describes a tradeoff analysis that can be done to select a suitable requirements elicitation method and the results of trying three methods in some case studies. It is a companion to the requirements elicitation introduction[3].
Requirements Elicitation Introduction	22.09.06 16:08:56	An area that is largely neglected is that of elicitation methods for security requirements engineering. Many organizations, if they use an elicitation method at all, use one that they have previously used for ordinary functional (end-user) requirements. Alternatively they may decide to use a brainstorming approach to identify security requirements. In many cases these methods are not oriented towards security requirements and do not result in a consistent and complete set of security requirements. The resulting system is likely to have more security exposures than it would if the requirements were elicited in a systematic way. In this article we briefly discuss a number of elicitation methods and the kind of tradeoff analysis

3. daisy:533 (Requirements Elicitation Introduction)

		that can be done to select a suitable requirements elicitation method. Companion case studies can be found in Requirements Elicitation Case Studies[4]. While results may vary from one organization to another, the discussion of our selection process and various methods should be of general use. Requirements elicitation is an active research area, and we expect to see advances in this area in the future. We also would expect that we will be able to begin to measure which methods are most effective for eliciting security requirements. At present, there is little if any data comparing the effectiveness of different methods for eliciting security requirements.
Requirements Engineering Annotated Bibliography	07.03.06 8:23:16	Abstracts and summaries from the source publications were used for the annotations in this bibliography.
Security Requirements Engineering	23.05.06 16:17:49	Security requirements are often identified during the system life cycle. However, the requirements tend to be general mechanisms such as password protection, firewalls, virus detection tools, and the like. As a result, security requirements that are specific to the system and that provide for protection of essential services and assets are often neglected. Several approaches to security requirements engineering are described that can help organizations ensure that their products effectively meet security requirements.
SQUARE Process	19.04.06 12:22:22	System Quality Requirements Engineering (SQUARE) provides a means for eliciting, categorizing, and prioritizing security requirements for

4. daisy:532 (Requirements Elicitation Case Studies Using IBIS, JAD, and ARM)

		information technology systems and applications. The focus of the methodology is to build security concepts into the early stages of the development life cycle. The model can also be used for documenting and analyzing the security aspects of fielded systems and for steering future improvements and modifications to those systems.
The Common Criteria	05.09.06 16:48:46	The Common Criteria enable an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements. Although the focus of the Common Criteria is evaluation, it presents a standard that should be of interest to those who develop security requirements.

####

###	########
Categories	best-practices